TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 USC 371

International Application No.:	PCT/AU00/00418
International Filing Date:	May 5, 2000
Priority Date Claimed:	May 6, 1999 and October 27, 1999
Title of Invention:	A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM
Applicant(s) for DO/EO/US:	Sydney Gordon Low and Peter Yandell

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

(X) This is a **FIRST** submission of items concerning a filing under 35 USC 371.

(X) This express request to begin national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 USC 371(b) and PCT Articles 22 and 39(1).

(X) A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

(X) A copy of the International Application as filed (35 USC 371(c)(2))

a) () is transmitted herewith (required only if not transmitted by the International Bureau).
b) (X) has been transmitted by the International Bureau.
c) () A copy of Form PCT/IB/308 is enclosed.
d) () is not required, as the application was filed in the United States Receiving Office (RO/US).

(X) Amendments to the claims of the International Application under PCT Article 19 (35 USC 371(c)(3))

e) () are transmitted herewith (required only if not transmitted by the International Bureau).
f) () have been transmitted by the International Bureau.
g) () have not been made; however, the time limit for making such amendments has NOT expired.
h) (X) have not been made and will not be made.

(X) A Declaration and Power of Attorney of the inventors (35 USC 371(c)(4)).

(X) A Notification of Transmittal of the International Preliminary Examination Report and a copy of the International Preliminary Examination Report with any annexes thereto, such as any amendments made under PCT Article 34.

(X) A FIRST preliminary amendment.

(X) International Application as published (with International Search Report).

(X) The present application qualifies for small entity status under 37 C.F.R. § 1.27.

(X) A return prepaid postcard.

(X) The following fees are submitted:

JC17 Rec'd PCT/PTO 23 JUL 2001

				FEES
	BASIC FEE			$860
CLAIMS	**NUMBER FILED**	**NUMBER EXTRA**	**RATE**	
Total Claims	32 - 20 =	12 ×	$18	$216
Independent Claims	13 - 3 =	10 ×	$80	$800
Multiple dependent claims(s) (if applicable)			$270	$0
	TOTAL OF ABOVE CALCULATIONS		$1,876	
Reduction by 1/2 for filing by small entity (if applicable). Verified Small Entity statement must also be filed. (NOTE 37 CFR 1.9, 1.27, 1.28)			$938	
	TOTAL NATIONAL FEE			$938
	TOTAL FEES ENCLOSED			$430

(X) A check in the amount of $430 to cover the above fees is enclosed.

(X) The Commissioner is hereby authorized to charge only those additional fees which may be required, now or in the future, to avoid abandonment of the application, or credit any overpayment to Deposit Account No. 11-1410.

SEND ALL CORRESPONDENCE TO:

John M. Carson
Reg. No. 34,303
Customer No. 20,995

H:\DOCS\MOH\MOH-5579.DOC:ad
071001

09/890002
518 Rec'd PCT/PTO 23 JUL 2001

Knobbe Martens Olson & Bear LLP
Intellectual Property Law

620 Newport Center Drive
Sixteenth Floor
Newport Beach, CA 92660
Tel 949-760-0404
Fax 949-760-9502
www.kmob.com

John M. Carson
619-687-8632
jcarson@kmob.com

Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Attorney Docket No.	:	DAVI130.001APC
Applicant(s)	:	Low, et al.
For	:	A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM
Attorney	:	John M. Carson
"Express Mail" Mailing Label No.	:	EL 707067258US
Date of Deposit	:	July 23, 2001

I hereby certify that the accompanying
Transmittal Form;
International Application as Published (with International Search Report);
Preliminary Amendment in 9 pages (with abstract on 1 page);
Notification of Transmittal of International Preliminary Examination Report with attached International Preliminary Examination Report;
SIGNED Declaration in 2 pages;
Check for Filing Fees;
Return Prepaid Postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Carol Macarty

H:\DOCS\MOH\MOH-5580 DOC ad
071001

09/890002
JC17 Rec'd PCT/PTO 23 JUL 2001

DAVI130.001APC

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Low, et al.	Group Art Unit Unknown
Appl. No.	:	Unknown	
Filed	:	Herewith	
For	:	A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM	
Examiner	:	Unknown	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Prior to examination of the above-captioned application, please amend the application as follows:

IN THE SPECIFICATION:

Please amend the specification as follows:

On page 1, line 2, please insert-- Field of the Invention --;

On page 1, line 5, please insert-- Background of the Invention --;

On page 1, line 30, please insert-- Summary of the Invention --;

On page 4, immediately before line 1, please insert--Brief Description of the Drawings --;

On page 4, line 10, please insert-- Detailed Description of the Invention --;

On page 13, line 1, please replace "Claims" with-- WHAT IS CLAIMED IS: --

IN THE ABSTRACT:

Please add an abstract submitted herewith on a separate page.

IN THE CLAIMS:

Please amend the following claims as indicated:

Please cancel Claims 1-26 without prejudice.

Please add the following new Claims:

27. An access system comprising:

connection means for connecting a computer device and establishing a connection session for accessing a public communications network;

switch means having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic receivable by the computer device; and

session managing means for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device.

28. The access system of Claim 27, wherein the session managing means is adapted to dynamically assign and adjust the access states during the session.

29. The access system of Claim 27, wherein the access states are defined by rules which determine locations of the network accessible by the computer device.

30. The access system of Claim 29, wherein the switch means is adapted to redirect the computer device to a predetermined network location based on the access state for the session.

31. The access system of Claim 27, wherein the session is a TCP/IP session and the connection data includes at least one of an IP address for the session and profile data stored in the system for a user of the computer device.

32. The access system of Claim 31, wherein the access requests include requests for TCP/IP data, and wherein the access state determines whether the computer device can receive the requested TCP/IP data.

33. The access system of Claim 32, wherein the TCP/IP data is one of the following: web pages, streaming audio, streaming video, interactive chat sessions, email and TFP sites.

34. The access system of Claim 27, wherein data available on the public communications network is partitioned based on the access states, and the session managing means is adapted to allocate the access states to different sessions handled by the switch means simultaneously and dynamically during each session.

35. The access system of Claim 34, wherein the session managing means includes a connection manager to manage connection and disconnection of each session, a session coordinator to establish a session manager for each session, and session managers for each session to process the access requests collected by the access system and assign access states for the sessions.

36. The access system of Claim 27, wherein the access states include an affiliate access state that restricts access to locations on the network affiliated with a provider of the access system.

37. The access system of Claim 27, wherein the access states include a portal state that connects the computer device to a predetermined portal page.

38. The access system of Claim 27, wherein the access states include a login state, a registration state, a general browsing state which allows access to all locations on the network, and an allow state which allows access to all locations on the network without the user of the computer device providing authentication data.

39. The access system of Claim 27, wherein the session managing means is adapted to allocate a number of the access states at respective times during the session.

40. The access system of Claim 39, wherein on disconnection of the session, the switch means reverts to the login access state.

41. An access system for public communications network, comprising:

means for connecting a computer device and establishing a TCP/IP session for access to the network;

switch means having a plurality of access states, the access states determining the sites and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the session.

42. A communication network access system, comprising:

connection means for receiving a request from a computer device to connect to a communications network and for connecting the computer device to the network in response to the request;

sending means for sending login data to the computer device after it is connected to the network, the login data being adapted to generate a login display on the computer device which allows entry of unique authentication data by a user of the device; and

login means for receiving the unique authentication data entered by the user and for allowing the user to access the network using the computer device upon determining that the authentication data is valid.

43. The system of Claim 42, wherein the connection means includes a switch having a set of access states enclosed therein and the login means accesses profile data for the user to control access to the network using the switch and the profile data to determine one of the access states for the switch.

44. The system of Claim 43, wherein the connection means includes a remote access server.

45. The system of Claim 44, wherein the sending means and login means include a web server and a user database.

46. A communications network access method, comprising:

establishing a TCP/IP session with a computer device; and

assigning access states during the session, the access states determining TCP/IP data received by the computer device.

47. A communications network access method, comprising:

connecting a computer device to a communications network;

accessing data from affiliate locations on the network without an access charge; and

accessing data from other locations on the network with an access charge.

48. A communications network access method, comprising:

receiving a request from a computer device to connect to a communications network;

connecting the computer device to the network in response to the request;

sending login data to the computer device after the connecting, the login data being adapted to generate a login display on the computer device allowing entry of unique authentication data by a user of the device;

receiving the unique authentication data entered on the computer device; and

allowing the user to access the network using the computer device when the authentication data is validated.

49. The method of Claim 48, additionally comprising accessing profile data for the user and controlling access to the network using the profile data.

50. The method of Claim 49, wherein the profile data determines one of a set of access states encoded in a switch connecting the computer device to the network.

51. The method of Claim 50, wherein the login display includes links to locations on the communications network for which entry of the authentication data is not required.

52. A communications network access method, comprising:

sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device, based on the login data, the display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network; and

obtaining access to the network after the authentication data is validated.

53. An access system comprising:

a connection device configured to connect a computer device and establish a connection session for accessing a public communications network;

a switching device having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic receivable by the computer device; and

a managing device configured to manage a session and assign at least one of the access states during the session based on connection data for the session and access requests from the computer device.

54. An access system for public communications network, comprising:

a connection device configured to connect a computer device and establish a TCP/IP session for access to the network;

a switching device having a plurality of access states, the access states determining sites and pages which can be accessed by the computer device during the session; and

a managing device configured to manage the session to allocate at least one of the access states during the session.

55. A computer readable program product comprising computer program code for accessing a communications network, said computer program code providing for execution of a method comprising:

establishing a TCP/IP session with a computer device; and

assigning access states during the session, the access states determining TCP/IP data received by the computer device.

56. A computer readable program product comprising computer program code for accessing a communications network, said computer program code providing for execution of a method comprising:

connecting a computer device to a communications network;

accessing data from affiliate locations on the network without an access charge; and

accessing data from other locations on the network with an access charge.

57. A computer readable program product comprising computer program code for accessing a communications network, said computer program code providing for execution of a method comprising:

receiving a request from a computer device to connect to a communications network;

connecting the computer device to the network in response to the request;

sending login data to the computer device after the connecting, the login data being adapted to generate a login display on the computer device allowing entry of unique authentication data by a user of the device;

receiving the unique authentication data entered on the computer device; and

allowing the user to access the network using the computer device when the authentication data is validated.

58. A computer readable program product comprising computer program code for accessing a communications network, said computer program code providing for execution of a method comprising:

sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device, based on the login data, the display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network; and

obtaining access to the network after the authentication data is validated.

REMARKS

The foregoing amendments are to more closely conform the application to U.S. practice. No new matter is added. Entry of the amendments is respectfully requested.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 7/23/01

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
620 Newport Center Drive
Sixteenth Floor
Newport Beach, CA 92660
(619) 235-8550

H:\DOCS\MOH\MOH-5515.DOC:ad
062701

ABSTRACT

An access system includes a connection device for connecting a computer device and establishing a connection session for accessing a public communications network, and a switch device having a plurality of access states. One of the access states is assigned to the session for at least part of the session. Each access state determines network traffic receivable by the computer device. The access system included further session managing means for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device.

P0259 "10060959

09/890002
JC17 Rec'd PCT/PTO 23 JUL 2001

A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

The present invention relates to a method and system for accessing a communications network, such as the Internet.

Most Internet users currently connect to the Internet via the equipment of an Internet service provider (ISP). The ISP provides remote access servers (RASs) which are able to communicate with remote computers of the users using modems and standard telephone lines. The remote computers and the RASs use standard software that executes a protocol, such as the point to point protocol (PPP), to allow the users to dial into the RASs and connect to the Internet. To achieve this, the connection or PPP software on the user's computer requires the user to enter unique authentication data, such as the user's login name and password, and this is transmitted to the ISP when the software dials and connects to the ISP equipment. If the ISP equipment determines that the authentication data is valid, the user's computer is connected and the user is allowed uninhibited access to the Internet. The user is accordingly free to view any desired web pages using a web browser on the user's computer.

The success of web sites on the Internet, particularly from a commercial perspective, is almost solely dependent on a site's ability to attract traffic to it. For this reason, a number of well known sites, such as Netscape's home page and the home pages of ISPs have been reconfigured to operate as communication "portals" to the Internet in the hope that users will continually revert to the sites to determine where to direct their browsers next. A number of sites have proved to be extremely lucrative, in the same manner as television stations which are able to attract large numbers of viewers. The current market value of companies such as Yahoo and Excite, which maintain high traffic volume sites, indicates how lucrative. As ISPs constitute a first point of connection for most Internet users, any steps or method which an ISP can implement to direct users to particular pages, rather than the user's own default home page, would be highly desirable. The present invention seeks to provide such method or at least provide a useful alternative.

In accordance with the present invention there is provided an access system including:

connection means for connecting a computer device and establishing a connection session for accessing a public communications network;

switch means having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic receivable by the computer device; and

session managing means for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device.

The present invention also provides an access system for a public communications network, such as the Internet, including:

means for connecting a computer device and establishing a TCP/IP session for access to the network;

switch means having a plurality of access states, the access states determining the sites and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the session.

The present invention also provides a communications network access system, including:

connection means for receiving a request from a computer device to connect to the network and for connecting the computer device to the network in response to the request;

sending means for sending login data to the computer device after it is connected to the network, the login data being adapted to generate a login display on the computer device which allows entry of unique authentication data by a user of the device; and

login means for receiving the unique authentication data entered by the user and for allowing the user to access the network using the computer device on determining that the authentication data is valid.

The present invention also provides a communications network access method, including:

PCT/AU00/00418 09.08.2000

establishing a TCP/iP session with a computer device: and

assigning access states during the session. the access states determining TCP/IP data received by the computer device.

The present invention also provides a communications network access method. including:

connecting a computer device to a communications network:

accessing data from affiliate locations on the network without an access charge: and

accessing data from other locations on the network with an access charge.

The present invention also provides a communications network access method. including:

receiving a request from a computer device to connect to the network;

connecting the computer device to the network in response to the request;

sending login data to the computer device after the connecting step, the login data being adapted to generate a login display on the computer device allowing entry of unique authentication data by a user of the device;

receiving the unique authentication data entered on the computer: and

allowing the user to access the network using the computer device when the authentication data is validated.

The present invention also provides a communications network access method. including:

sending a request from a computer device to connect to a communications network. and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device. based on the login data. the display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network: and

obtaining access to the network after the authentication data is validated.

A preferred embodiment of the present invention is hereinafter described, by way of example only with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of a communications network access system;

Figure 2 is a block diagram of a server system of the access system;

Figure 3 is a flow diagram of a communications network access method of the access system;

Figure 4 is a diagram of a login page of the system and method; and

Figure 5 is a diagram of a customised home page of the system and method.

A communications access system, as shown in Figure 1, includes a plurality of remote access servers (RASs) 4, a layer four or higher switch 6, a database server 8, a web server system 10 and a router 12. The RASs 4 are provided to allow the computers 14 of remote users to dial into the system using standard telecommunication lines and modems and connect to the input ports of the RASs 4, respectively. On connection to a port of a RAS 4, the RAS 4 and the user's computer 14 establish a unique TCP/IP session and the IP traffic for that session is switched by the switch 6. Once the user is authenticated or approved, as described below, the user's computer 14 is allowed to access requested data on the Internet 16. The web server system 10 is used to control pages presented to a user 14 connected to the RAS 4 and handle authentication using a member profile database maintained on the database server 8, as described below. A RADIUS (Remote Authentication Dial In User Service) authentication server 11 is also provided for use in authentication. As far as the user 14 is concerned, the equipment 4, 6, 8, 10, 11 and 12 of the access system is part of the Internet.

The equipment 4 to 12 preferably includes standard commercially available hardware and basic database, web server and Internet access software which is known to those skilled in the art and is used in the access systems of most ISPs. The equipment 4 to 12 then also includes unique program code to manage and control each session, as discussed below. The layer four or higher switch 6 is another exception. The switch 6 is normally used by ISPs to balance the traffic handled by the RASs 4. An example of a suitable layer four switch is the AceDirector AD3™ produced by Alteon WebSystems Inc. The access system differs from that

offered by ISPs, as described below, in that the layer four switch 6 is used to connect users to the web server system 10 and control access to the Internet 16 for the users 14 on the basis of a limited number of access states encoded in the switch 6. Alternatively the unique program code and the equipment 4 to 12 could be substituted, entirely or in part, by unique integrated circuits, such as ASICs, to execute the same functions.

The switch 6 controls access to the Internet 16 by assigning an access state to each TCP session, as identified by a respective IP address. The states are each defined by one or more access rules which are encoded in the switch 6. The rules define how the switch 6 is to direct IP traffic by executing pattern matching on the received traffic. For example, the states may include a login state, a portal state, a general state, an affiliate state, a registration state, and an allow state, as described below. A rule, for example, may be receive a first URL and redirect to a second URL or the rules may allow or deny access to a predetermined set or list of URLs. The state assigned to a given IP address is controlled by a control system 20, as shown in Figure 2. The web server system 10 includes the control system 20 and a web server 22, running Apache™, which maintains web pages for the access system.

When the user 14 wishes to connect to the Internet using the access system, the user 14 dials into the system using standard PPP software and is allocated a port at the RAS 4 which answers the call. On connecting to a RAS 4, the user 14 is assigned an IP address for the IP session. The IP address is allocated from an IP address pool which depends on the number which the user dialled to connect to the RAS 4. For example, the user may have a dial-in number which provides the user with free access to Internet web sites as part of a promotion, and the user 14 is assigned an IP address and port which signifies to the switch 6 that all traffic from that IP address is to be switched directly to the router 12 and out to the Internet 16. This would occur with all IP addresses within this pool being allocated to the allow state of the switch 6, described below. Other IP addresses assigned by the RASs 4 are initially allocated to a login state of the switch until the state is changed by the control system 20. Traffic with IP addresses assigned to the login state is all redirected to the control system 20 by switch 6.

The control system 20, as shown in Figure 2, includes a RADIUS accounting server 30, a login server 32, a session coordinator 34, individual session managers 36, an authentication client 38, a redirector server 42 and a plan manager 44. The components 30 to 44 are all software components, but can if desired be partly or entirely replaced by application specific integrated circuits (ASICs). The control system 20 is configured to handle three different authentication scenarios:

(i) Legacy authentication using the RADIUS authentication server 11.

(ii) Authentication using a login display, e.g. browser based authentication.

(iii) No authentication required.

For the first scenario, the user 14 dials into the RASs 4 using standard PPP software and provides a username and password. Based on the dial in number used and the configuration of the PPP software, the RAS port assigned to handle the call will direct the data provided to the RADIUS authentication server 11 to authenticate the user based on the PPP username and the password. Once authenticated, the RADIUS authentication server 11 returns a connect status message to the RAS 4 and an IP address is assigned to the user. Based on the IP address, the switch 6 forwards from the RAS 4 the connect status message, the username, calling line identification (CLI) and the IP address to the control system 20. This data is processed by the RADIUS accounting server 30 which acknowledges the new connection for the IP address and accesses the database server 8 to record the connection time for the user. The RADIUS accounting server 30 acknowledges and monitors all connections and disconnections for IP addresses, and issues connection and disconnection messages to other components in the access system. The session coordinator 34 uses the connection data, together with profile data accessed from the member profile database for the user 14, to create an instance of a session manager 36 for the connection. The connection data passed to the session coordination 34 in the connect message includes the IP address, the username and the CLI. Session managers 36 are created for each connection or session, respectively, and provide instructions to the redirector server 42 to control the state at the switch 6 for the session.

A session manager 36 controls the traffic which the user can receive during the session by controlling the state of the switch 6 for the user's IP address. The state control is executed

on the basis of the user's member profile held in the member profile database of the server 8. The profile specifies which one of a limited number of access profiles the user belongs to. The access profiles each contain data which defines the access states that the user is able to enter. The different access states are encoded in the switch 6. On authentication of a TCP/IP session the session manager 36 for the session instructs the redirection server 42 to store data in the switch 6 indicating which one of the access states apply to the session. For example, during authentication the session is in a login state and can change to a general state or affiliate state once authentication has been completed.

In the second authentication scenario, the access system executes browser based authentication using the access procedure shown in Figure 3. The user is able to connect to the Internet by simply dialling into the access system using standard PPP software, at step 62, and the RASs 4 will automatically connect the user 14 without requiring the entry of any username or password. The user is automatically connected, an IP address assigned and a TCP session established, when the user dials into a port of a RAS 4 using predetermined call numbers. The system informs the user's computer 14 of the connection and the PPP software will display for the user the fact that the connection has been established and any other details associated with the connection, such as the data rate. The IP address is assigned from an address pool for immediate connection.

Once the user is connected to the access system the switch 6 determines whether the user's machine 14 is requesting connection to another computer on the Internet 16, at step 64. The request for example, may be simply to the user's default home page when the user opens a web browser of the computer 14. The switch 6 then determines, at step 66 by checking a stored flag representing the switch state for the IP address, whether the user has been authenticated and that the state is not the login state. If the connection session is in the login state, the switch 6 connects the user 14 to a login page on the web server 22, and the control system 20 executes a login process 68. The login process 68 is similar to that for legacy authentication, in that the RAS accounting server 30 acknowledges that connection has occurred and a new session has been established for the IP address. Data for the session is passed to the session coordinator 34 to create an instance of a session manager 36 for the

session. Based on the IP address, however, the session manager 36 determines that the user needs to be authenticated using browser based authentication and accordingly waits for the login server 32 to receive from the web server 22 details submitted on the login page shown in Figure 4. The login page presents the user with a number of options, which includes executing a registration process to become a new registered user, entering a username and password if already registered, or accessing help pages stored on the server 22. The page also includes a number of banner advertisements which may include links to other pages or web sites. To gain general access to the Internet 16, however, the user must enter a valid username and password combination which is authenticated by the control system 20. The login page allows the user to enter a username and password combination and then send the combination for authentication by clicking on the "sign in" button. Alternatively the combination may already be stored on the computer 14 by the user. The username and password combination is received by the session manager 36 for the session and the combination is forwarded to the authentication client 38. The authentication client 38 passes the combination to an authentication daemon 40 running on the database server 8. The authentication daemon checks the combination against stored combinations for users to determine if it is valid, identify the user and access the unique member profile for the user from the database server 8.

In the third authentication scenario, no authentication is required. In this scenario the user is allocated a telephone number to dial in on which corresponds to no authentication. The user is automatically connected, as for browser based authentication, and assigned an IP address from a pool for no authentication. Operation proceeds as described above for browser based authentication, except that the session manager 36 does not revert to the authentication client 38 to authenticate the user based on a username and password combination. The user is simply authenticated automatically by the session manager 36.

Once the user has been authenticated, either by the login process 28 or using the RADIUS server 11, an individual session manager 36 uses the member profile data for the user to compile and send a customised home page, as shown in Figure 5 to the user 14. The customised home page may also include banner advertisements, in the same manner as for the login page. The session manager 36 instructs the redirector server 42 to change the state of the

switch 6 to a portal state, after authentication, which directs the switch to connect to the URL for the customised home page or portal shown in Figure 5. Details concerning the user and customised home page data from the member profile are passed by the session manager 36 to the login server 32 for access by the Apache server 22 which controls compilation of the customised home page. Subsequently, the session manager 36 instructs the redirector server so as to divert the switch to one of the browsing states, either an affiliate state or a general state. For browser based authentication, as shown in Figure 3, the login authentication process is managed using the web browser of the user's machine 14, rather than the PPP software, and operation returns after the login process 68 to step 64. Accordingly, once the user reverts to step 64 and is determined at step 66 as having been authenticated, the switch 6 determines at step 70, on the basis of the access state for the session, whether the user is allowed to access a requested computer or service. If so, the user is granted access to the computer or service on the Internet 16 at step 62. If not, the user 14 is advised at step 64 of the access denial. The access denial can be communicated by connecting the user to a denial page of the Apache server 22.

A user 14 having a session which is in the affiliate state is allowed access, at no charge, to sites maintained by affiliates of the provider of the access system. The affiliate sites may be maintained on the Apache server 22 or on other servers of the Internet 16. The affiliate sites are all identified by URLs in the rules of the affiliate state. The affiliate sites can also be accessed using the links provided in the web pages of Figures 4 and 5. The rules for the affiliate state specify that access is denied to any URLs which do not belong to the affiliate sites. If however a user has a member profile that allows access to other sites on the Internet, the user is able to move to the general state. For these users, when a request is made to access a site other than an affiliate site, the user's browser is redirected by the switch 6 to an interim blank page on the Apache server 22 while the session manager 36 determines whether to instruct the redirector server 42 to change the state of the switch to the general state. The interim blank page contains code to trap the requested URL and pass the URL and a message to the login server 32 advising that the user is attempting to move from the affiliate state to the general state. This message is passed to the session manager 36, on the basis of the IP address, and the session manager 36 accesses the member's profile. If the session manager 36

determines on the basis of the profile that the user 14 is allowed to move the general state, a message is sent to the redirector server 42 to change the state of the switch to the general state for the session. A message is also sent from the manager 36 to the login server 32 advising that the user 14 is allowed to move to the trapped URL. The login server 32 sends a message to the Apache server 22 to forward the user 14 from the interim page to the page of the requested trapped URL. If access is denied, the URL of a denied page is used to substitute the trapped URL at the login server 32, and the user 14 is forwarded to the denial page.

Other access states are the registration state and the allow state. A session manager 36 will instruct the redirector server 42 to enter the switch 6 into the registration state for a session when a user sends a message indicating they wish to register with the access system. This may be done when, for example, the user selects the registration option on the login page of Figure 4. In the registration state the switch 6 redirects the user 14 to registration pages on the Apache server 22 and the control system 20 collects the requested details on the pages from the user 14 for the user file in the database server 8. The user file normally includes the member profile data for the user which is initially established on the basis of the requested details. A session manager 36 will instruct the redirector server to cause the switch 6 to enter the allow state when the IP address indicates that the user 14 is to be provided with unrestricted access to the Internet 16 without any monitoring or charge.

When the session is disconnected, the RAS 4 communicates disconnection to the RADIUS accounting server 30, which in turn advises the session manager 36. The manager 36 instructs the redirector server 42 to change the state of the switch 6 to the login state for the IP address of the disconnected session.

The manner in which the user is charged is controlled by a plan manager 44 that is accessed by the session manager 36. The plan manager 44 maintains different charging plans which can be applied to users. For example, all users would not be charged for access to affiliate sites, but the rate of charge may differ for accesses when in the general state. For instance, users may be allocated a predetermined period of free access for pages to the general state and then charged at a set rate thereafter. The plan manager specifies the times and rates

for the different plans, and this is accessed by the session managers 36 which monitor the time a user spends in different access states. The ultimate charge for a session is compiled by the session managers 36 and then stored against the user's file in the database server 8.

In addition to the hardware and software configuration variations for the access system discussed above, the operations executed by the switch 6 can be implemented by the following different system configurations. Firstly, the switch 6 can be replaced by a layer four switch and a proxy server. The layer four switch redirects all traffic from the RASs 4 to the proxy server which is connected to the router 12. The proxy server is also connected to the control system 20. The proxy server 10 is used to establish the different access states for each connection session, with the states being dynamically adjusted under the control of the control system 20. The proxy server also stores the rules defining each of the access states which it can provide for different sessions. Another alternative, instead of encoding the access states in the switch 6, is to provide software control logic with the switch 6 to define the different access states and store the associated rules for the states, and thereby handle redirection of traffic to the web server 22 or a proxy server, as required, depending on the access state and access requests made. The control logic communicates with the control system 20, as discussed above, to dynamically adjust the access states for different sessions.

The access method and system are particularly advantageous as they allow ISPs, at least initially, to dynamically control the pages viewed by a user. As a minimum, the user must, and cannot avoid, viewing the login or customised home page, as these are an integral part of the login process. This allows the ISP to present advertising information, and in particular present targeted advertising information based on the user's profile, which the ISP can guarantee that all of its users will not be able to avoid. The login and customised home pages therefore act as an entry portal for all users.

By also allowing all users to connect to the system, including users who are not registered, the ISP is able to present and provide free access to selected and predetermined Internet content and services. For example, the login page may include links to certain web pages that provide banking, stock trading or home shopping, and the user will not have to pay

any fees to the ISP to access these pages. This allows the ISP to act as a free content provider for certain content, whilst charging a user to access other data on the Internet. To provide information to advertisers associated with the free content, the ISP can, if desired, still require and obtain certain information on and from users before providing the free content, and monitor their access.

Encoding the access states in the switch 6 also allows the ISP to restrict or allow access to selected content or services on the Internet, such as sports betting, adult orientated content or children's content.

Many modifications will be apparent for those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

CLAIMS:

1. An access system including:

connection means for connecting a computer device and establishing a connection session for accessing a public communications network;

switch means having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic receivable by the computer device; and

session managing means for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device.

2. An access system as claimed in claim 1, wherein the session managing means is adapted to dynamically assign and adjust the access states during the session.

3. An access system as claimed in claim 1, wherein the access states are defined by rules which determine locations of the network accessible by the computer device.

4. An access system as claimed in claim 3, wherein the switch means is adapted to redirect the computer to a predetermined network location based on the access state for the session.

5. An access system as claimed in claim 1, wherein the session is a TCP/IP session and the connection data includes an IP address for the session and/or profile data stored in the system for a user of the computer device.

6. An access system as claimed in claim 5, wherein the access requests include requests for TCP/IP data, such as web pages, streaming audio and video, interactive chat sessions, e-mail or FTP sites, and the access state determines whether the computer device can receive the requested TCP/IP data.

7. An access system as claimed in claim 1, wherein data available on the public communications network is partitioned based on the access states, and the session managing means is adapted to allocate the access states to different sessions handled by the switch means simultaneously and dynamically during each session.

8. An access system as claimed in claim 7, wherein the session managing means includes a connection manager to manage connection and disconnection of each session, a session coordinator to establish a session manager for each session, and session managers for each session to process the access requests collected by the access system and assign access states for the sessions.

9. An access system as claimed in claim 1, wherein the access states include an affiliate access state that restricts access to locations on the network affiliated to a provider of the access system.

10. An access system as claimed in claim 1, wherein the access states include a portal state that connects the computer device to a predetermined portal page.

11. An access system as claimed in claim 1, wherein the access states include a login state, a registration state, a general browsing state which allows access to all locations on the network, and an allow state which allows access to all locations on the network without the user of the computer device providing authentication data.

12. An access system as claimed in claim 1, wherein the session managing means is adapted to allocate a number of the access states at respective times during the session.

13. An access system as claimed in claim 11, wherein on disconnection of the session, the switch means reverts to the login access state.

14. An access system for a public communications network, such as the Internet, including:

means for connecting a computer device and establishing a TCP/IP session for access to the network;

switch means having a plurality of access states, the access states determining the sites and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the session.

15. A communications network access system, including:

connection means for receiving a request from a computer device to connect to the network and for connecting the computer device to the network in response to the request;

sending means for sending login data to the computer device after it is connected to the network, the login data being adapted to generate a login display on the computer device which allows entry of unique authentication data by a user of the device; and

login means for receiving the unique authentication data entered by the user and for allowing the user to access the network using the computer device on determining that the authentication data is valid.

16. A communications network access system as claimed in claim 15, wherein the connection means includes a switch having a set of access states encoded therein and the login means accesses profile data for the user to control access to the network using the switch and the profile data to determine one of the access states for the switch.

17. A communications network access system as claimed in claim 16, wherein the connection means includes a RAS.

18. A communications network access system as claimed in claim 17, wherein the sending means and login means includes a web server and a user database.

19. A communications network access method, including:

establishing a TCP/IP session with a computer device; and

assigning access states during the session, the access states determining TCP/IP data received by the computer device.

20. A communications network access method, including:

connecting a computer device to a communications network;

accessing data from affiliate locations on the network without an access charge; and

accessing data from other locations on the network with an access charge.

21. A communications network access method, including:

receiving a request from a computer device to connect to the network;

connecting the computer device to the network in response to the request;

sending login data to the computer device after the connecting step, the login data being adapted to generate a login display on the computer device allowing entry of unique authentication data by a user of the device;

receiving the unique authentication data entered on the computer; and

allowing the user to access the network using the computer device when the authentication data is validated.

22. A communications network access method as claimed in claim 21, including accessing profile data for the user and controlling access to the network using the profile data.

23. A communications network access method as claimed in claim 22, wherein the profile data determines one of a set of access states encoded in a switch connecting the computer device to the network.

24. A communications network access method as claimed in claim 23, wherein the login display includes links to locations on the communications network for which entry of the authentication data is not required.

25. A communications network access method, including:

sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device, based on the login data, the display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network; and

obtaining access to the network after the authentication data is validated.

26. Computer software including code for executing the steps of the method as claimed in any one of claims 19 to 25.

PCT/AU00/00418 09.06.2000

10/05/2001 09:00:03

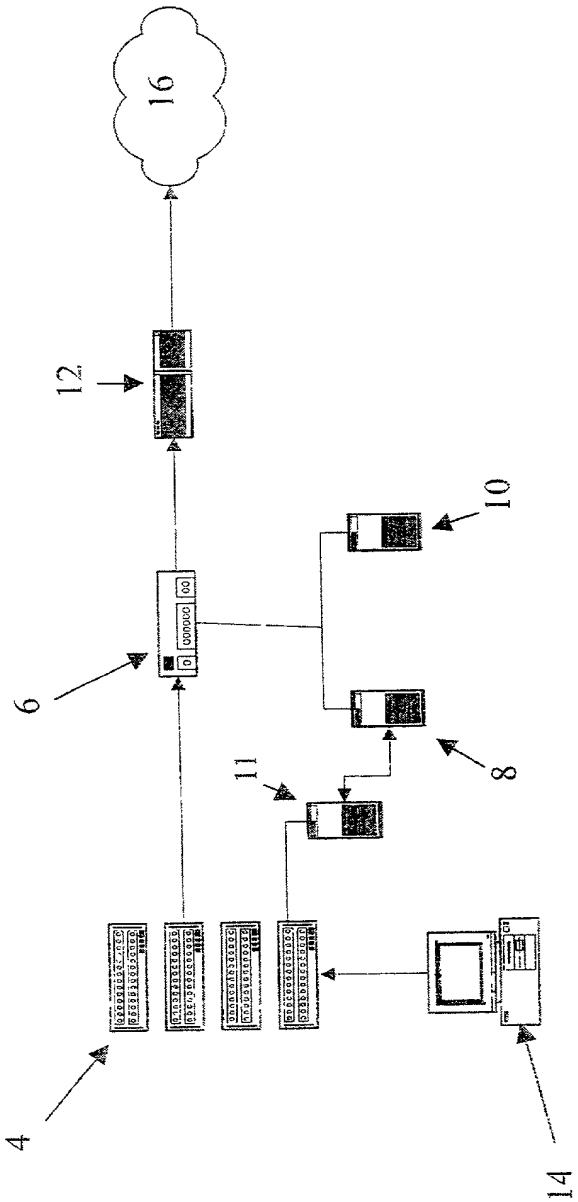


Figure 1

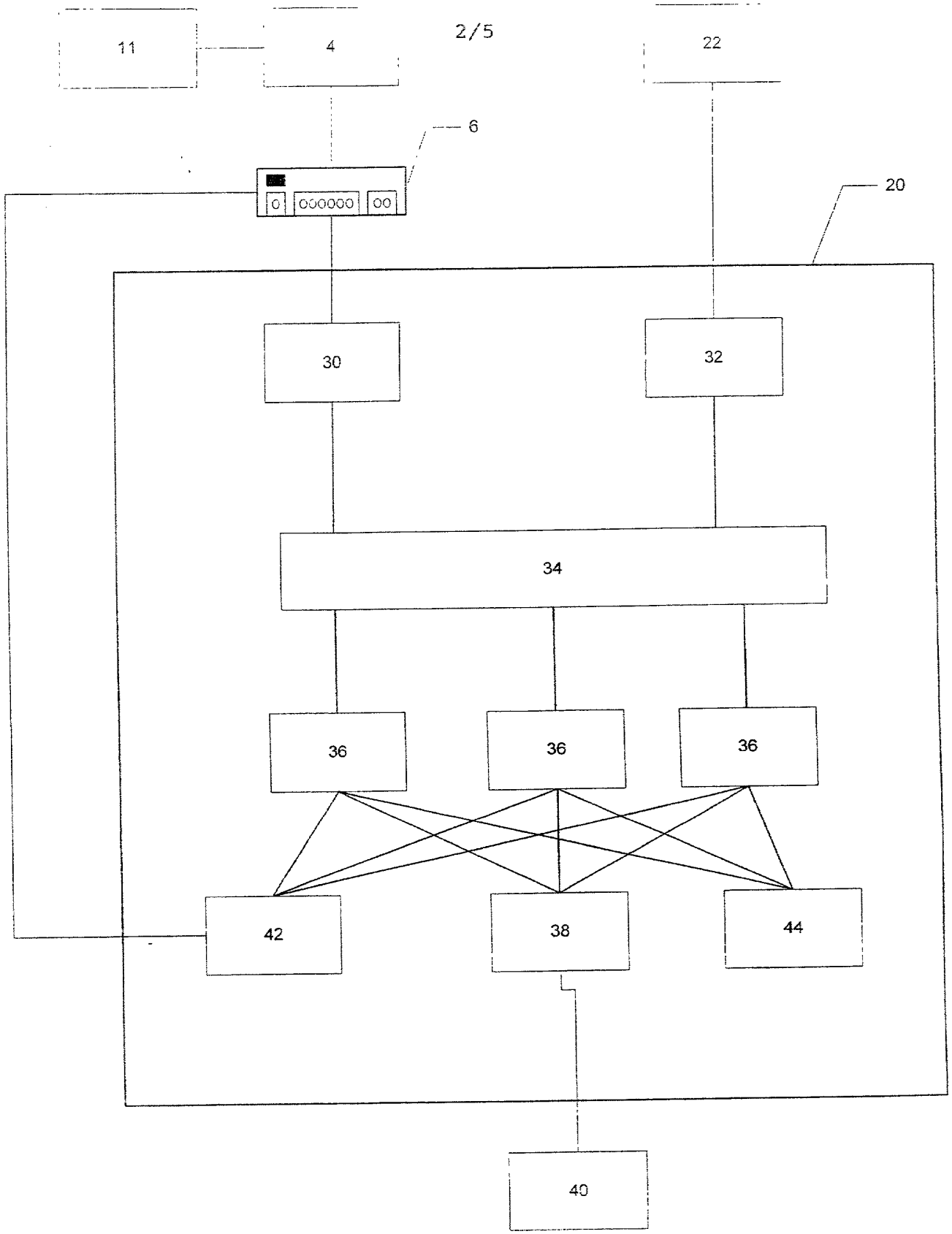
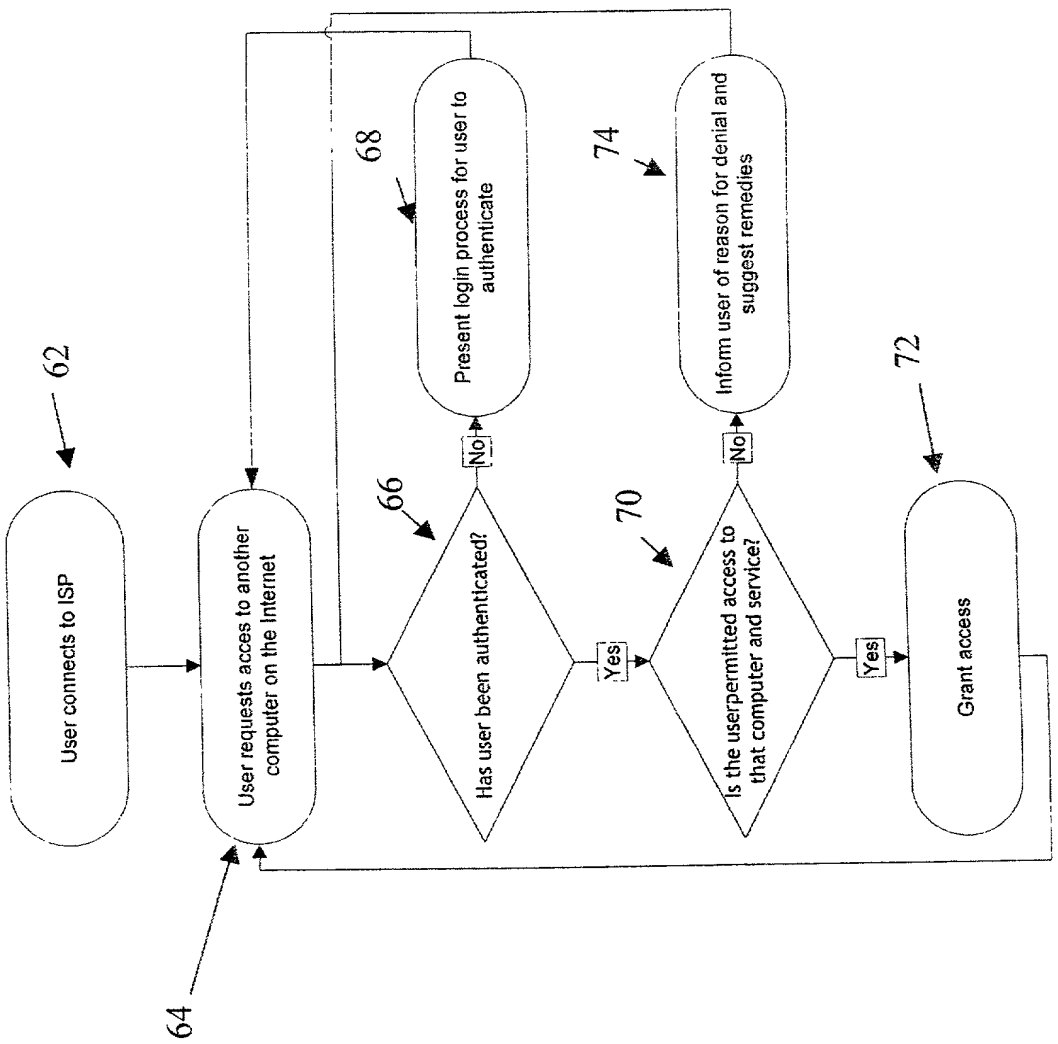


Figure 2

Figure 3


60
62
User connects to ISP
64
User requests acces to another computer on the Internet
66
Has user been authenticated?
No
68
Present login process for user to authenticate
Yes
70
Is the userpermitted access to that computer and service?
No
74
Inform user of reason for denial and suggest remedies
Yes
72
Grant access

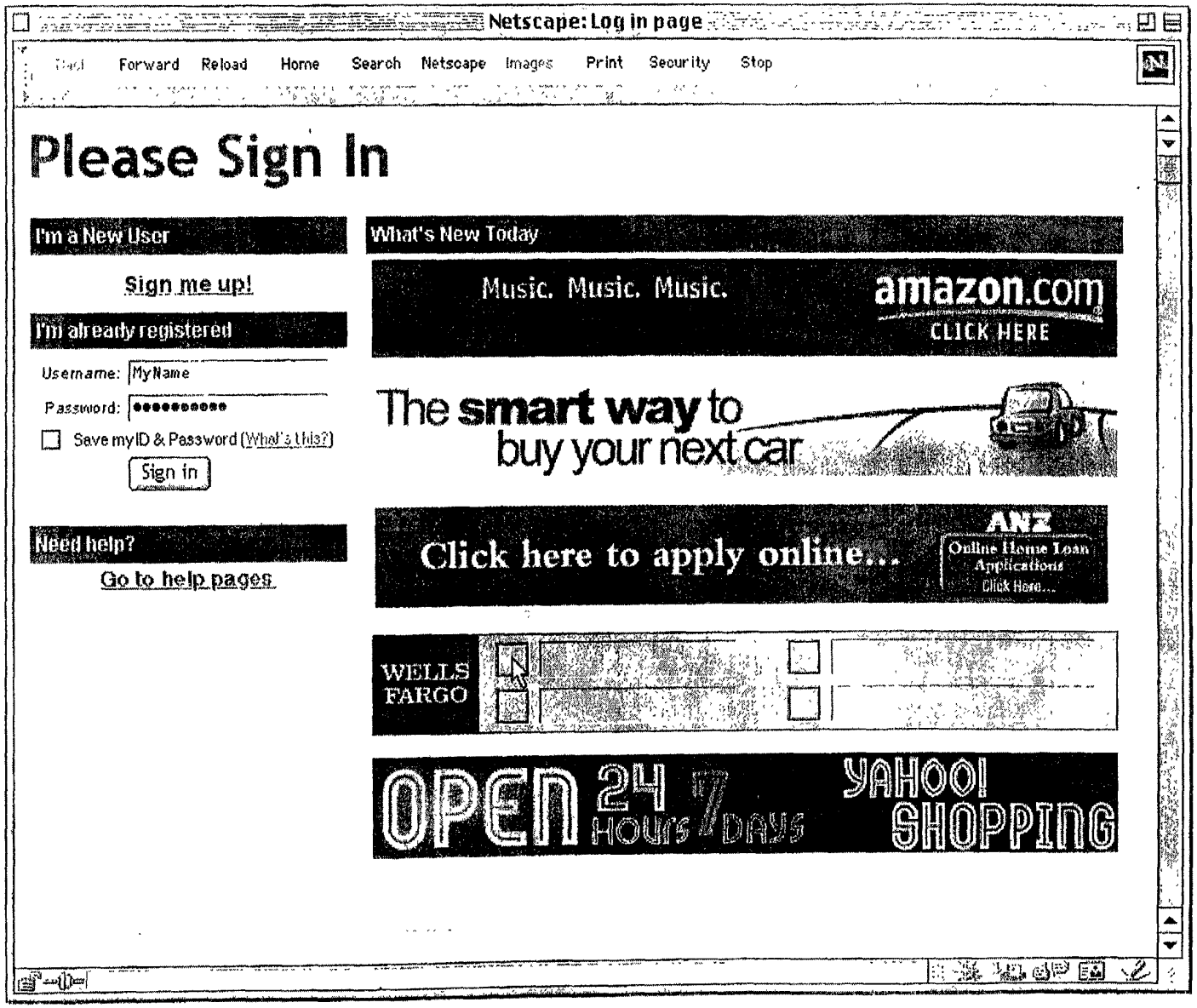


Figure 4

WO 00/68862
4/5
09/890002
PCT/AU00/00418

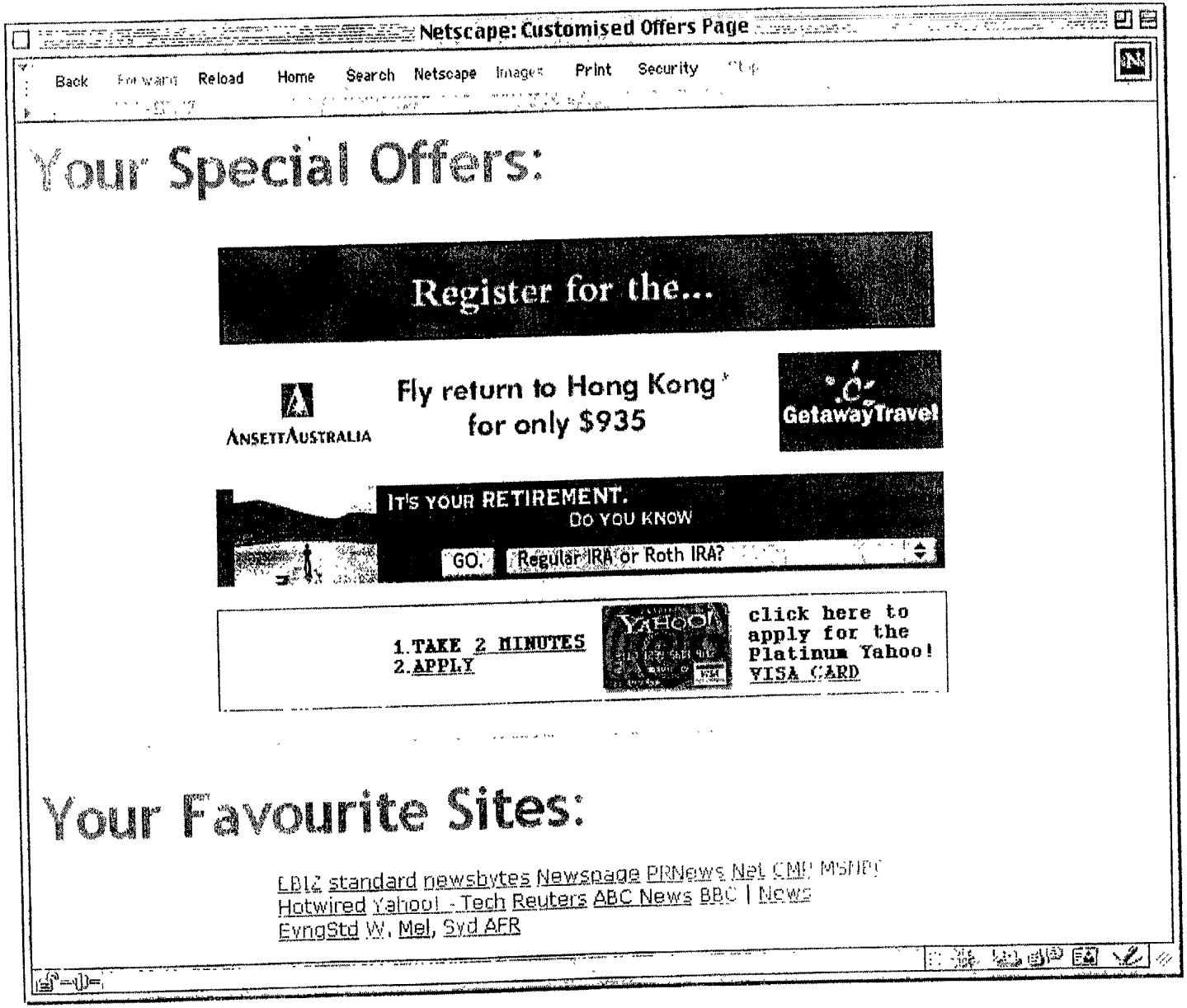


Figure 5

WO 00/68862
PCT/AU00/00418

09/890002

DECLARATION AND POWER OF ATTORNEY - USA PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

the specification of which:

(a) ☐ is attached hereto; or

(b) ☐ was filed on _____ as ☐ Application No. 0 /_____ or ☐ Express Mail No., as Application No. not yet known _____ and was amended on _____ (if applicable); or

(c) ☒ was described and claimed in PCT International Application No. PCT/AU00/00418 filed on 5 May, 2000 and as amended under PCT Article 19 on _____ (if any) and/or under PCT Article 34 on 21 February, 2001 (if any).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above;

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56;

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent, design or inventor's certificate or any PCT international application(s) listed below and have also identified below any foreign application(s) for patent, design or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed for the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 U.S.C. § 119
Australia	PQ0213/99	6 May, 1999	☒ YES NO ☐
Australia	PQ3682/99	27 October, 1999	☒ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this application:

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(714) 760-0404 FAX (714) 760-9502

Prior U.S.A. Application(s)

Application No.: _____ Filing Date: _____ Status: _____

POWER OF ATTORNEY: I hereby appoint the registrants of Knobbe, Martens, Olson & Bear, LLP, 620 Newport Center Drive, Sixteenth Floor, Newport Beach, California 92660, Telephone (714) 760-0404, **Customer No. 20,995**, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith (if this application is assigned, I acknowledge that the appointed individuals do not represent me, and that instead they represent the assignee).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

1-00

Full name of sole or first inventor: Sydney Gordon LOW

Inventor's signature _____ Day 21 Month MAY Year 2001

Residence (city and country): Kew, Victoria, Australia AUX

Citizenship: Australian

Post Office Address: 9 Evans Road, Kew, Victoria 3101, Australia

2-00

Full name of second inventor: Peter YANDELL

Inventor's signature _____ Day 18 Month 5 Year 2001

Residence (city and country): Belgrave, Victoria, Australia AUX

Citizenship: Australian

Post Office Address: 39 Best Street, Belgrave, Victoria 3160, Australia

Full name of third inventor: _____

Inventor's signature _____ Day ___ Month _____ Year _____

Residence (city and country): _____

Citizenship: _____

Post Office Address: _____

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20,995